The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/27/2019

SUBJECT:
A Vulnerability in Apple iOS Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Apple iOS, which could allow for arbitrary code execution. Apple iOS is a mobile operating system for mobile devices, including the iPhone, iPad, and iPod touch. Successful exploitation of this vulnerability could result in arbitrary code execution with system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- iOS versions prior to 12.4.1

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: HIGH

TECHNICAL SUMMARY:

A vulnerability has been discovered in Apple iOS, which if exploited could allow for arbitrary code execution with system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The vulnerability exists due to a use-after-free error. Specifically, this issue occurs due to stale pointer left by 'in6_pcbdetach()' function.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.

- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:
Apple:
https://support.apple.com/en-us/HT210549

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8605

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov